# Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ ○ TLP:WHITE Alert ID : e4cf95fd Jun 28, 2023, 09:31 AM

This week, *Hacking Healthcare*™ takes a broad look at what is going on in the world of Artificial Intelligence (AI) policy and lawmaking. After briefly examining the European Union's (EU) AI Act and the current state of AI policy in the United States (US), we break down how the various approaches being taken may impact healthcare and cybersecurity.

Additionally, *Hacking Healthcare*™ will be off next week for a quick summer vacation, but we will return the following week with more in-depth analysis.

## AI Policy Update

The interest in AI and Machine Learning (ML) has exploded in the past year as maturing tools like ChatGPT, Bard, Midjourney, and DALL-E have found mainstream popularity. This surge of interest, occasionally punctuated with fears of AI sentience and risks to human existence, has largely highlighted the lack of clear laws and regulations in this space.[i], [ii] This week, *Hacking Healthcare* strives to provide a high-level overview of where the US and EU are on AI policies, strategies, laws, and regulations. Our analysis section will examine how these approaches intersect with the Healthcare and Public Heath (HPH) sector and cybersecurity.

### EU: Leading the way

The EU is perhaps the furthest along when it comes to setting out clear laws and regulations for AI tools and applications, and their flagship legislation on this matter is the AI Act. Initially presented in the Spring of 2021, the AI Act is working its way through the latter portion of the EU's legislative process and is likely to be "the world's first rules on Artificial Intelligence."[iii], [iv]

The EU's framework, as outlined in the AI Act, attempts to strike a balance between the benefits and risks of AI and is guided by the following intentions:[v]

- AI systems placed and used on the Union market are safe and respect existing law on fundamental rights and Union values;
- Ensure legal certainty to facilitate investment and innovation in AI;
- Enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- Facilitate the development of a single market for lawful, safe, and trustworthy AI applications and prevent market fragmentation.

The bulk of the AI Act outlines how AI systems are to be regulated according to an assessment of their risk. AI systems will fall into one of three categories:

- Prohibited: AI systems and practices deemed to be too harmful, likely too harmful, or those that stray from established EU laws, rights, and values are to be prohibited outright. This category is expected to include things like real-time use of biometric identification, predictive policing, emotion recognition, and social scoring.

- High-Risk: AI systems and practices that are deemed to be High-Risk, either through meeting certain conditions outlined in the text or as identified in Annex III, are allowable, provided they conform to range of requirements.[vi] These requirements include elements of data governance, transparency, documentation, human oversight, and cybersecurity. Annex III includes the category *Management and operation of critical infrastructure*.

- Non-High-Risk: AI systems and practices that do not fall under the first two categories are encouraged, but not mandated, to conform to the requirements placed on those in the high-risk category.

The AI Act is meant to be a flexible and “future proof” piece of legislation and is designed to complement the growing constellation of EU technology and cybersecurity laws and regulations, such as the Digital Services Act (DSA), Cyber Resilience Act (CRA), Network Information and Information Security (NIS2) Directive, General Data Protection Regulation (GDPR), and EU market based New Legislative Framework (NLF).

The EU is currently working through a reconciliation process where the various bodies negotiate text amendments leading to the final version of the law. Expectations are that this process will wrap up by the end of the year, with implementation expected to take roughly two years after that.

US: Catching Up

The US has lagged behind the EU when it comes to regulating emerging technology in general, and AI appears is no different. Despite being a hotbed of technological innovation and having previously put out noteworthy signaling documents on AI, like the Biden Administration’s *Blueprint for an AI Bill of Rights*, US policymakers have yet to make serious inroads on actual law and regulation.[vii]

While there has been a number of proposals put forward on numerus aspects and use cases for AI, a consensus comprehensive and coherent approach has yet to emerge. Most recently, Senator Schumer [D-NY] discussed a high-level framework that “[called] for an approach to A.I. prioritizing objectives like security, accountability and innovation.”[viii] The lack of specifics appears to be an acknowledgement that much of the US Congress lacks significant expertise on the issue, and that time might be needed to educate members before a serious effort gets underway.

*Action & Analysis*
****Included with Health-ISAC Membership****

***Congress***

Tuesday, June 27
No relevant hearings

Wednesday, June 28
No relevant meetings

Thursday, June 29

No relevant meetings

***International Hearings/Meetings***

No relevant meetings

[i] https://www.npr.org/2022/06/16/1105552435/google-ai-sentient

[ii] https://www.nytimes.com/2023/05/30/technology/ai-threat-warning.html#:~:text=%E2%80%9CMitigating%20the%20risk%20of%20extinction,AI%20Safety%2C%20a%20nonprofit%20organization.

[iii] https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

[iv] https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

[v] https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

[vi] https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF

[vii] https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf

[viii] https://www.nytimes.com/2023/06/21/us/ai-regulation-schumer-congress.html

**Report Source(s)**

Health-ISAC

**Reference | References**

**Europa Analytics**<br>
**NPR**<br>
**Health-ISAC**<br>
**New York Times**<br>
**Europa Analytics**<br>
**Europa Analytics**<br>
**New York Times**<br>
**Whitehouse**

**Tags**

Regulation, Hacking Healthcare, Policy, Artificial Intelligence, law, European Union

**TLP:WHITE:** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

**Conferences, Webinars, and Summits:**

**https://h-isac.org/events/**

**Hacking Healthcare:**

Written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House.  John is currently the Senior Director of Cybersecurity Services at Venable.  His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

### Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

### For Questions or Comments:

Please email us at toc@h-isac.org